Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) An apparatus ~~for providing a computer security firewall~~, comprising:

~~an ASIC including~~ a firewall engine including: ~~with~~

a first engine including a first set of rules for sorting incoming IP packets into initially allowed packets and initially denied packets;[[,]] and

a filter including a second set of rules for receiving and further sorting the initially denied packets into allowed packets and denied packets.

2. (Original) The apparatus of claim 1, wherein the filter dynamically generates the second set of rules.

3. (Original) The apparatus of claim 2, wherein the first set of rules comprises fixed rules.

4. (Original) The apparatus of claim 3, further comprising:

a second engine for receiving and further processing the initially allowed packets.

5. (Original) The apparatus of claim 4, wherein the second engine is capable of modifying some subset of the initially allowed packets.

6. (Currently Amended) The apparatus of claim 5, wherein the second engine comprises:

a dynamic analyzer for identifying initially allowed packets requiring network address translation[[,]]; and

a handler for providing network address translation.

7. (Original) The apparatus of claim 5, wherein the second engine comprises a dynamic analyzer for sending a "reset" packet to a source IP address.

8. (Currently Amended) A computer software product, tangibly stored on a computer-readable medium, for providing ~~a~~ network security ~~firewall~~, comprising instructions operable to cause a programmable processor to:

~~computer code for sorting~~ process incoming IP packets into initially allowed packets and initially denied packets;

~~computer code for extracting~~ extract matching criteria from incoming IP packets;

~~computer code for~~ dynamically ~~generating~~ generate rules using the extracted matching criteria; and

~~computer code for~~ further ~~sorting~~ process the initially denied packets using the dynamically-generated rules.

a4

9. (Currently Amended) The computer software product of claim 8, wherein the instructions to ~~computer code for sorting~~ process incoming IP packets ~~uses~~ use fixed rules.

10. (Currently Amended) The computer software product of claim 9, further comprising instructions to:

~~computer code for~~ further ~~sorting~~ process the initially allowed packets into allowed packets and packets requiring modification.

11. (Currently Amended) The computer software product of claim 10, further comprising instructions to:

~~computer code for modifying~~ modify control packets.

12. (Currently Amended) The computer software product of claim 11, wherein the instructions to ~~computer code for modifying~~ modify control packets ~~includes computer code~~ include instructions for network address translation.

a2

13. (Currently Amended) The computer software product of claim 10, further comprising instructions to:

~~computer code for generating~~ generate and ~~transmitting~~ transmit a "reset" packet in response to a denied packet.

14. (Currently Amended) A method for providing network computer security, comprising:

receiving incoming ~~IP~~ packets at a firewall;

sorting the incoming ~~IP~~ packets into initially allowed packets and initially denied packets; and

a4 further sorting the initially denied packets into allowed and denied packets using ~~dynamically-generated~~ rules.

15. (Currently Amended) The method of claim 14, wherein the step of sorting the incoming ~~IP~~ packets is performed using fixed rules.

16. (Original) The method of claim 15, further comprising the step of further sorting the initially allowed packets into allowed packets and packets requiring modification.

17. (Original) The method of claim 16, further comprising the step of providing network address translation for packets requiring modification.

20
~~18.~~ (Original) A method for providing network computer security, comprising:

receiving incoming IP packets at a firewall;

sorting the incoming IP packets into initially allowed packets and initially denied packets using a set of fixed rules;

extracting parameters from the incoming IP packets;

using the extracted parameters to generate a set of dynamically-generated rules; and

further sorting the initially denied packets into allowed and denied packets using the dynamically-generated rules.

21 20

~~19~~. (Original) The method of claim ~~18~~, further comprising the step of further sorting the initially allowed packets into allowed packets and packets requiring modification.

22 21

~~20~~. (Original) The method of claim ~~19~~, further comprising the step of providing network address translation for packets requiring modification.

18

~~21~~. (New) The method of claim 14, wherein the packets are IP packets.

19

~~22~~. (New) The method of claim 14, wherein the rules are dynamically generated.

a4

23. (New) An apparatus comprising:

an ASIC including a firewall engine including:

a first engine including a first set of rules for processing incoming IP packets into initially allowed packets and initially denied packets; and

a filter including a second set of rules for receiving and further processing the initially denied packets into allowed packets and denied packets.

24. (New) A method for providing network computer security, comprising:

receiving incoming packets at a firewall;

processing the incoming packets into initially allowed packets and initially denied packets; and

further processing the initially denied packets into allowed and denied packets using rules.

Amendments to the Drawings:

In Figures 1-7b, the figures have been formalized.

Attachments following last page of this Amendment:

Replacement Sheet (Abstract: 1 page, Formal drawings: 6 pages)